(19) JAPANESE PATENT OFFICE

PATENT ABSTRACTS OF JAPAN

(11) Publication number: **2002063063 A**

(43) Date of publication of application: **28.02.02**

(51) Int. Cl **G06F 12/00**
G06F 12/14

(21) Application number: **2001167946**

(22) Date of filing: **04.06.01**

(30) Priority: **05.06.00 JP 2000167482**

(71) Applicant: **FUJITSU LTD**

(72) Inventor: **IWATANI SAWAO**

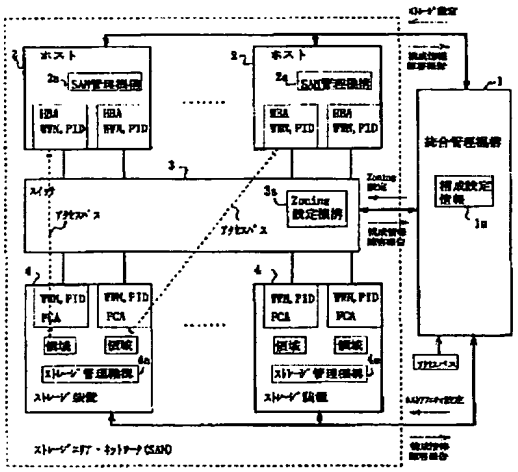
(54) STORAGE AREA NETWORK MANAGING SYSTEM

(57) Abstract:

PROBLEM TO BE SOLVED: To automatically perform best security management for a SAN(storage area network) by unitarily integrating/managing conventional discrete security methods.

SOLUTION: An integrating/managing mechanism 1 for integrating/managing SAN is installed, so that access relations between hosts 2 and storage devices 4 can be collectively managed by using the managing mechanism 1. Access paths, that is, areas on the storage device 4 side which are to be accessed from the host 2 side, and fiber channel adaptors(FCAs) and host bus adaptors(HBAs), which are used when the storages are accessed, are set in the mechanism 1. Based on access path information set, the mechanism 1 performs storage settings, a zoning setting, and settings for which area to permit access, for SAN managing mechanism 2a of the hosts 2, a zoning setting mechanism 3a of a switch 3, and storage managing mechanisms 4a of the storage devices 4, respectively.

本発明の概要を説明する図



(19)日本国特許庁（ＪＰ）　(12)公開特許公報（Ａ）　(11)特許出願公開番号
特開2002－63063
（P2002－63063A）
(43)公開日　平成14年２月28日(2002.2.28)

(51)Int.Cl.[7]	識別記号	ＦＩ		テーマコード（参考）
Ｇ０６Ｆ　12/00	５４５	Ｇ０６Ｆ　12/00	５４５Ｂ	５Ｂ０１７
	５３７		５３７Ａ	５Ｂ０８２
12/14	３２０	12/14	３２０Ａ	

審査請求　未請求　請求項の数９　ＯＬ　（全 20 頁）

(21)出願番号　特願2001－167946(P2001－167946)
(22)出願日　平成13年６月４日(2001.6.4)
(31)優先権主張番号　特願2000－167482(P2000－167482)
(32)優先日　平成12年６月５日(2000.6.5)
(33)優先権主張国　日本（ＪＰ）

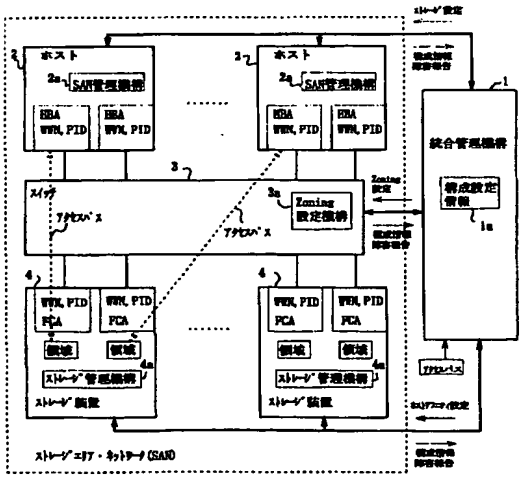
(71)出願人　000005223
富士通株式会社
神奈川県川崎市中原区上小田中４丁目１番１号
(72)発明者　岩谷　沢男
神奈川県川崎市中原区上小田中４丁目１番１号　富士通株式会社内
(74)代理人　100100930
弁理士　長澤　俊一郎　（外１名）

Ｆターム(参考)　5B017 AA03 BA06 CA07
5B082 EA11

(54)【発明の名称】　ストレージエリア・ネットワーク管理システム

(57)【要約】
【課題】　従来の分割されたセキュリティ方式を一元的に統合管理し、ＳＡＮにおいて最善のセキュリティ管理を自動的に行うこと。
【解決手段】　ＳＡＮを統合制御する統合管理機構１を設置し、ホスト２とストレージ装置４とのアクセス関係をこの管理機構１を用いて一括して管理できるようにする。統合管理機構１にアクセスパス、すなわち、ホスト２側からアクセスをしようとするストレージ装置４側の領域と、そのストレージをアクセスする際の使用するファイバチャネルアダプタ（ＦＣＡ）、ホストバスアダプタ（ＨＢＡ）を設定する。設定されたアクセスパス情報を元に、統合管理機構１は、ホスト２のＳＡＮ管理機構２ａ、スイッチ３のゾーニング(Zoning)設定機構３ａ、ストレージ装置４のストレージ管理機構４ａに、それぞれストレージ設定、ゾーニング設定、アクセスをどこの領域に対して許可するかの設定を行う。

本発明の概要を説明する図



1

【特許請求の範囲】

【請求項１】　複数のホストコンピュータと複数のストレージ装置が、スイッチを介して接続されたストレージエリア・ネットワーク・システムにおいて、

上記ストレージエリア・ネットワークを統合制御する統合管理機構を備え、該統合管理機構はホストコンピュータとストレージ装置とのアクセス経路情報を備えるとともに、該アクセス経路情報に基づき、ホストコンピュータのストレージエリア・ネットワーク管理機構に対して、ストレージ装置に対する管理情報を通知し、スイッチの領域設定機構に対して領域情報を通知し、ストレージ装置のストレージ管理機構に対して上記ホストコンピュータについてのアクセス制限情報を通知することを特徴とするストレージエリア・ネットワーク管理システム。

【請求項２】　上記統合管理機構は、ストレージエリア・ネットワークの構成状態を個々の装置より取得して、ストレージエリア・ネットワークの構成設定情報として保持し、

定期的もしくは、システム管理者からの指示によって、現状のストレージエリア・ネットワークの構成状態を集収し、上記構成設定情報と集収した現状の構成情報とを比較することにより、ストレージエリア・ネットワーク・システムの異常を判断することを特徴とする請求項１のストレージエリア・ネットワーク管理システム。

【請求項３】　上記統合管理機構は、ホストコンピュータのストレージエリア・ネットワーク管理機構、スイッチ、および／またはストレージ装置より、アクセス関係情報を取得して、アクセスパスの整合性を確認し、アクセスパスが正しく設定されていないとき、その部分を異常として通知することを特徴とする請求項１または請求項２のストレージエリア・ネットワーク管理システム。

【請求項４】　複数のホストコンピュータと複数のストレージ装置が、スイッチを介して接続され、これらを統合管理する統合管理機構を備えたストレージエリア・ネットワーク・システムにおけるホストコンピュータであって、

上記ホストコンピュータのストレージエリアネットワーク管理機構は、上記統合管理機構から通知されるストレージ装置に対する管理情報に基づきストレージ装置に対するアクセス情報を設定することを特徴とするストレージエリア・ネットワーク・システムにおけるホストコンピュータ。

【請求項５】　複数のホストコンピュータと複数のストレージ装置が、スイッチを介して接続され、これらを統合管理する統合管理機構を備えたストレージエリア・ネットワーク・システムにおけるスイッチであって、

上記スイッチの領域設定機構は、上記統合管理機構から通知される領域情報に基づき領域設定を行うことを特徴とするストレージエリア・ネットワーク・システムにおけるスイッチ。

2

【請求項６】　複数のホストコンピュータと複数のストレージ装置が、スイッチを介して接続され、これらを統合管理する統合管理機構を備えたストレージエリア・ネットワーク・システムにおけるストレージ装置であって、

上記ストレージ装置のストレージ管理機構は、上記統合管理機構から通知されるアクセス制限情報に基づき、ストレージに対するアクセス制限条件を設定することを特徴とするストレージエリア・ネットワーク・システムにおけるストレージ装置。

【請求項７】　複数のホストコンピュータと複数のストレージ装置が、スイッチを介して接続されたストレージエリア・ネットワーク・システムを統合管理する統合管理機構であって、

上記統合管理機構は、ホストコンピュータのストレージエリア・ネットワーク管理機構に対して、ストレージ装置に対する管理情報を通知し、スイッチの領域設定機構に対して領域情報を通知し、ストレージ装置のストレージ管理機構に対して上記ホストコンピュータについてのアクセス制限情報を通知することを特徴とするストレージエリア・ネットワーク・システムにおける統合管理機構。

【請求項８】　複数のホストコンピュータと複数のストレージ装置が、スイッチを介してファイバチャネルで接続されたストレージエリア・ネットワーク・システムを統合制御する統合管理プログラムであって、

上記統合管理プログラムは、ホストコンピュータとストレージ装置とのアクセス経路情報に基づき、ホストコンピュータのストレージエリア・ネットワーク管理機構に対して、ストレージ装置に対する管理情報を通知する処理と、

スイッチの領域設定機構に対して領域情報を通知する処理と、ストレージ装置のストレージ管理機構に対して上記ホストコンピュータについてのアクセス制限情報を通知する処理とをコンピュータに実行させ、

ホストとストレージとのアクセス関係を一括して管理することを特徴とするストレージエリア・ネットワーク・システムを統合制御するプログラム。

【請求項９】　複数のホストコンピュータと複数のストレージ装置が、スイッチを介してファイバチャネルで接続されたストレージエリア・ネットワーク・システムを統合制御する統合管理プログラムを記録した記録媒体であって、

上記統合管理プログラムは、ホストコンピュータとストレージ装置とのアクセス経路情報に基づき、ホストコンピュータのストレージエリア・ネットワーク管理機構に対して、ストレージ装置に対する管理情報を通知し、スイッチの領域設定機構に対して領域情報を通知し、ストレージ装置のストレージ管理機構に対して上記ホストコ

ンピュータについてのアクセス制限情報を通知し、ホストとストレージとのアクセス関係を一括して管理することを特徴とするストレージエリア・ネットワーク・システムを統合制御するプログラムを記録した記録媒体。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】本発明はファイバチャネル・ネットワークを用いて複数のサーバ／複数のストレージを結合するストレージエリア・ネットワーク（以下ＳＡＮと呼ぶ）の管理システムに関する。

【０００２】

【従来の技術】近年、１台のストレージ・システムの容量が大きくなり、複数の多種多様なサーバから使用できるような機能が求められている。また、データ転送経路に高速かつ複数ホスト・ストレージ間の並列転送が可能なファイバチャネルが普及し始めたことをきっかけに、この環境での接続形体はさらに大規模化すると考えられている。このような複数のサーバ／複数のストレージ結合をストレージエリア・ネットワーク（以下ＳＡＮという）と呼び、分散化されつつある複数サーバのストレージの一元的管理やＴＯＣの削減を計ろうする試みが進みつつある。

【０００３】

【発明が解決しようとする課題】しかしながら、ストレージ内の領域管理や、セキュリティの面で解決しなければならない問題がある。その一つに、ＳＡＮが複数のホストコンピュータ（以下ホストという）及び複数のストレージ・システムより構成されていた場合に、全てのホストから全てのストレージ・システムがアクセス可能である為に、あるホストから使用しているストレージ内のデータが他のホストから不用意に破壊されてしまう可能性があった。

【０００４】ストレージ内の領域管理や、セキュリティの面で完全な対策となるものがないのが現状である。また、ＳＡＮを構成する複数装置で障害が発生した際、いろいろなエラー報告がシステム管理者に報告される為、被疑箇所を特定することが難しく方法がなかった。本発明は上記事情を考慮してなされたものであって、本発明の目的は、従来の分割されたセキュリティ方式を一元的に統合管理し、ＳＡＮにおいて最善のセキュリティ管理を自動的に行うことができるようにすることである。

【０００５】

【課題を解決するための手段】図１は本発明の概要を説明する図である。同図に示すように、本発明は上記ＳＡＮ環境に対して、ＳＡＮを統合制御する統合管理機構１を設置し、ホスト２とストレージ装置４とのアクセス関係をこの管理機構１を用いて一括して管理できるようにする。システム管理者は、統合管理機構１にホスト２側からアクセスをしようとするストレージ装置４側の領域と、そのストレージをアクセスする際の使用するファイバチャネル・アダプタ（ＦＣＡ）、ホストバス・アダプタ（ＨＢＡ）を設定する。この設定をアクセスパスと呼ぶ。設定されたアクセスパス情報を元に、この統合管理機構１は、まずホスト２側から見えるストレージ設定（Storage affinity）をホスト２側のＳＡＮ管理機構２ａに設定する。また、スイッチ３のゾーニング(Zoning)設定機構３ａに対して、ＦＣＡ，ＨＢＡが保有するWWN，ＰＩＤ情報を事前に確保しておきこれを元に設定されたアクセスパスが実現できるように計算してゾーニング(Zoning)を設定する。さらに、ストレージ装置４のストレージ管理機構４ａには、ストレージ装置のどのＦＣＡがどこのＨＢＡ（WWN，ＰＩＤ）のアクセスをどこの領域に対して許可するかの設定を行う。上記のような統合管理機構１を設けることにより、ＳＡＮにおいて、セキュリティ管理やストレージ内の領域管理を一括して行うことができる。また、上記統合管理機構に、ＳＡＮの構成状態を構成設定情報１ａとして保持させることにより、ＳＡＮに、ＳＡＮ管理機能を持たないホストや、ゾーニング設定機能を持たないスイッチや、あるいはストレージ管理機能を持たないストレージ装置が投入されても容易に対応することができ、可能な範囲でセキュリティを確保することができる。

【０００６】さらに、上記統合管理機構１を設けることにより、以下の機能を実現することができる。

（１）統合管理機構１が、ＳＡＮの構成状態を個々の装置より確保して、構成設定情報１ａとして格納し、定期的もしくは、システム管理者からのコマンド指示によって、統合管理機構１が、現状のＳＡＮの構成状態を読込み、ＳＡＮの構成設定情報１ａと比較し、異なっていた場合は、異常と判断し、システム管理者に通知する。これにより、システム管理者はＳＡＮの異常を容易に知ることができる。

（２）統合管理機構１が、システム管理者からのコマンド指示によって、ＳＡＮ管理機構２ａ、Ｚｏｎｉｎｇ設定機構３ａ、ストレージ管理機構４ａよりアクセス関係情報を確保してアクセスパスの整合性を確認する。アクセスパスが正しく設定されていない場合は、その部分を異常とシステム管理者に通知する。これにより、システム管理者はアクセスパスの整合性を確認することができる。

（３）ホスト２、ホスト２のＨＢＡ、スイッチ３、あるいは、ストレージ装置３のＦＣＡが交換されたとき、上記統合管理機構１はこれを検知し、ホスト２のＳＡＮ管理機構２ａ、スイッチ３のゾーニング設定機構３ａ、もしくは、ストレージ装置４のストレージ管理機構４ａから、交換後の設定情報を取得し、交換前と同等のアクセス関係を構築するように再度アクセス関係を設定する。これにより、ＳＡＮの構成変更に対して容易に対処することができる。

（４）システム起動時にアクセスパスが設定されていな

い状態時に、スイッチ３に対して全てのアクセスを許可しない設定を行う。これにより、システム起動時にアクセスパスを設定していない状態で、不用意なアクセスが設定されることを防ぐことができる。

（５）ファイバチャネルではＨＢＡとＦＣＡ側で共通に設定すべきファイバチャネルの転送クラス(Class）というパラメータがある。このパラメータがＨＢＡ側とＦＣＡ側で異なっていると転送ができない。そこで、前記したアクセスパスを設定する際に、使用する転送クラスもシステム管理者に指定させて、統合管理機構１がＳＡＮ管理機構２ａ、ストレージ管理機構４ａを通じて、アクセスパスを設定したＨＢＡとＦＣＡが指定された同一の転送クラスで動作させる。これにより、転送クラスが異なることにより転送できないという不具合を解消することができる。

（６）ＳＡＮ内で障害が発生した場合は、まず、その障害報告を統合管理機構１が受け取り、システム管理者への報告を一端止める。規定時間他の障害が統合管理機構１が管理している装置から報告されていないかどうかを待ち合わせする。待ち合わせをしている間に受け取った障害報告に関しては中身をチェックし、最初に受け取った障害との関連性がないかを統合管理機構１が保持している各アダプタのWWN，ＰＩＤやアクセスパス情報から確認する。確認結果、関連すると判断された場合は、予め統合管理機構１内で設定されている障害報告方法定義に従って、一つのみの障害をシステム管理者に報告する。システム管理者は、この情報を元に迅速に被疑箇所を特定することができる。

（７）１つの被擬箇所と報告するだけでなく、関連して報告された被擬箇所と判定されなかった報告も、関連障害として報告する。これにより、影響範囲をシステム管理者は特定することができる。

（８）予め、統合管理機構１に、各アクセスパスの設定情報だけでなく各アクセスパスで使用しているホスト２側の論理ボリュームの情報もホスト２側のＳＡＮ管理機構２ａから確保し、統合管理機構１の構成設定情報１ａに格納しておく。統合管理機構１は、ＳＡＮ内から障害が報告されると、その故障箇所を使用しているアクセスパスを統合管理機構１内の構成設定情報１ａから取り出し、そのアクセスパスを使用しているホスト論理ボリュームを取り出し、障害影響のある論理ボリュームをシステム管理者に報告する。障害影響のある論理ボリュームが分かると、すぐに、その論理ボリュームのリカバリを行うことができ、業務に対する影響を最小限に止めることができる。

【０００７】

【発明の実施の形態】図２に本発明の対象となるＳＡＮシステムの構成例を示す。同図に示すように、ＬＡＮ（ローカルエリア・ネットワーク）に複数台のホストコンピュータ（以下ホストという）Ｈ－１～Ｈ－ｎと、後述するＳＡＮ総合管理機構として機能する管理サーバＳと、前述したスイッチＳＷ－１～ＳＷ－ｍ、ストレージ装置ＳＴ、磁気テープ装置ＭＴ等が接続される。ＳＡＮ（ストレージエリア・ネットワーク）は、ホストＨ－１～Ｈ－ｎ、スイッチＳＷ、ストレージ装置ＳＴ、磁気テープ装置ＭＴ等で構成されており、各ホストＨ－１～Ｈ－ｎ、スイッチＳＷ－１～ＳＷ－ｎ、ストレージ装置ＳＴ、磁気テープ装置ＭＴの間にはデータ転送路が設けられ、該データ転送路を介して各ホストＨ－１～Ｈ－ｎからストレージ装置ＳＴ等へのアクセスが行われる。また、ＬＡＮを介してＳＡＮの構成状態を示す情報等が管理サーバＳに伝送されるとともに、管理サーバＳからの各種設定情報等が各ホストコンピュータＨ－１～Ｈ－ｎ、スイッチＳＷ、ストレージ装置ＳＴ等に伝送される。

【０００８】図３は本発明の実施例のストレージエリア・ネットワーク・システムの構成を示す図である。ここでは、一例としてＳＡＮが、ホスト１１０、１２０、スイッチ３００、ストレージ装置４１０，４２０から構成されている場合について説明する。図３において、ホスト１１０，１２０はホストバス・アダプタ（以下ＨＢＡという）１１１，１１２，１２１を介してファイバチャネルでスイッチ３００と接続されており、ストレージ装置４１０，４２０はファイバチャネル・アダプタ（以下ＦＣＡという）４１１，４１２，４２１を介してスイッチ３００と接続されている。図４に図３に示すストレージ装置のハードウェア構成例を示す。同図において、サブシステム制御部１１はチャネルＩ／Ｆ部を介して上位装置に接続されており、サブシステム制御部１１はメモリ１１ａ、ＭＰＵ１１ｂ、バスインタフェース部１１ｃを備えており、上記ＭＰＵ１１ｂはメモリ１１ａに格納されているプログラムに従って動作する。また、メモリ１１ａには、プログラムの他に、転送データや制御データが格納される。

【０００９】１３はデバイス制御部であり、デバイス制御部１３は、バッファ１３ａ、ＭＰＵ１３ｂ、上記ＭＰＵ１３ｂを動作させるプログラム等を格納したメモリ１３ｃ、バスインタフェース部１３ｄを備えている。上記サブシステム制御部１１とデバイス制御部１３はバスＢＵＳを介して接続されており、デバイス制御部１３はデバイスＩ／Ｆ部１４を介してディスクドライブ群１５に接続される。

【００１０】上記ＳＡＮ環境に対して、本実施例では、ＳＡＮを統合制御する管理機構５００（前記図２の管理サーバＳがこの機能を持つ）を設置し、ホスト１１０，１２０とストレージ装置４１０，４２０とのアクセス関係をこの管理機構５００を用いて一括して管理できるようにする。また、この管理機構５００からの制御に対応させる為、ホスト側１１０，１２０にはＳＡＮ管理機構１１８，１２８を設置し、また、ストレージ装置４１

０，４２０にはストレージ管理機構４１８，４２８を設置する。

【００１１】ＳＡＮ管理機構とは前記ａ）で説明したストレージ・アフィニティの設定を行える機構であり、ストレージ管理機構は前記したｃ）で説明したホスト・アフィニティの設定が行える機構である。さらに、スイッチ３００には前記ｂ）で説明したスイッチのゾーニング設定機構３０１が搭載される。システム管理者は、ＳＡＮ統合管理機構５００にホスト側からアクセスをしようとするストレージ側の領域と、そのストレージをアクセスする際の使用するＦＣＡ（ファイバチャネル・アダプタ），ＨＢＡ（ホストバス・アダプタ）を設定する。この設定をアクセスパスの設定と呼ぶ。設定されたアクセスパス情報は、このＳＡＮ統合管理機構５００の中で、図５（ａ）に示すＳＡＮ統合管理機構５００内アクセスパス設定情報の様に格納される。この設定情報を元に、まずホスト側から見えるストレージ設定(Storage affinity)をホスト側のＳＡＮ管理機構１１８，１２８に設定する。すなわち、どのＨＡＢからどのＦＣＡ（WWN，ＰＩＤ）へのアクセスを行うかを設定する。

【００１２】また、どのＨＢＡからどのＦＣＡに対してアクセスするかの設定は、図５（ｂ）に示すストレージ・アフィニティ（Storage Affinity）テーブルのような管理テーブルをホスト内で作成し、アクセスするＦＣＡを選択させる事で実現する。この例では、ＨＢＡ１１１からWWNｃのＦＣＡに対して領域４１５をアクセスするように設定している。ファイバチャネル上のコマンドは、相手ＦＣＡのWWNを介して発行する事が出来る。さらに、スイッチ３００のゾーニング（Zoning）設定機構３０１に対して、ＦＣＡ，ＨＢＡが保有するWWN，ＰＩＤ情報を事前に確保しておき、これを元に設定されたアクセスパスが実現できるように計算してゾーニング（Zoning）を設定する。図５（ｃ）にスイッチ・ゾーニング（Zoning）テーブルの例を示す。ここではゾーン（Zone）をＡとＢで設定し、それぞれのゾーン（Zone）に相互アクセスを許可するポート（ＨＢＡ，ＦＣＡ）の識別子（ここではWWN）を格納する。これにより、スイッチWWNａからアクセスはゾーン（Zone）Ａと認識し、WWNｃに対してのみしか実行できないようなアクセス制限を行う。

【００１３】ファイバチャネル環境ではスイッチ３００とポートを接続するとログインシーケンスが動作し、その中でスイッチはポートのWWN情報を確保できる。この情報を元に、ホスト１１０，１２０からストレージ装置４１０，４２０にコマンドが発行された場合に、ゾーン（Zone）設定されていないポートに対するアクセスが指定された時、ストレージ装置４１０，４２０のポートにコマンドが伝わらないような制御を行う。さらに、ストレージ装置４１０，４２０のストレージ管理機構４１８，４２８には、ストレージ装置４１０，４２０のどのＨＢＡ，ＰＩＤからのアクセスを、何処の領域に対して許可するかの設定を行う。図５（ｄ）にホスト・アフィニティ（Host affinity ）テーブルの例を示す。このテーブルにより、ＦＣＡ４１１はWWNａのＨＢＡからのアクセスのみを領域４１５に対して許可し、ＦＣＡ４１２はWWNｅのＨＢＡからのアクセスのみを領域４１６に対して許可する。

【００１４】ファイバチャネル環境ではホストからのコマンドを受け付ける前に、ログインシーケンスという相互のポートの情報をやりとりするシーケンスがあり、その中で相手のWWNやＰＩＤなどを確認できる。ＦＣＡは、ここで確保した相手のWWNやＰＩＤの情報がアクセス許可されているものかどうかを判断し、アクセス許可がされたものに対してのみ処理を継続し、アクセス許可されていないものからのアクセスに対しては、チェックコンディション（Check condition ）等でエラー応答を行う。なお、ＳＡＮを構成するホスト装置のなかにはＳＡＮ管理機構をもたない装置がある。また、ストレージ装置内でも前記c)のホスト・アフィニティ機能を提供していない装置もある。したがって、そのような装置に対して管理機構５００はアクセス関係を設定しないが、他のセキュリティ方式(Storage Affinity もしくはZoning))によってセキュリティは保護される。

【００１５】図６によりＳＡＮ統合管理機構５００が行う作業のフローチャートとその作業の具体例を説明する。まず、ＳＡＮ統合管理機構５００は、各ＦＣＡ、ＨＢＡのWWN及びＰＩＤを読み込む（ステップＳ１）。図３の例においては、ＳＡＮ統合管理機構５００が例えばホスト１１０のＨＢＡ１１１がWWNａ，ＰＩＤａであり、ストレージ装置４１０のＦＣＡ４１１がWWNｃ，ＰＩＤｃ、ＦＣＡ４１２がWWNｄ，ＰＩＤｄ等であることを認識する。ついで、ＳＡＮ統合管理機構５００は、ＨＢＡからアクセスする予定のＦＣＡと、その配下の領域を受け付ける（ステップＳ２）。図３の例においては、例えばホスト１１０のＨＢＡ１１１からストレージ装置４１０のＦＣＡ４１１経由で領域４１５にアクセスするパス設定を受け付ける。

【００１６】次に、当該ホストがストレージ・アフィニティ(Storage Affinity)機能をサポートしているかを調べる（ステップＳ３）。ストレージ・アフィニティ(StorageAffinity)機能をサポートしていない場合にはステップＳ５に行く。また、ストレージ・アフィニティ(Storage Affinity)機能をサポートしている場合にはステップＳ４において、ストレージ・アフィニティ(Storage Affinity)機能により、ＳＡＮ統合管理機構５００は、ホスト側のＳＡＮ管理機構に、ＨＢＡからアクセスできるデバイスをWWNもしくはＰＩＤを使用して設定する。例えば図３の例においては、ホスト１１０のＨＢＡ１１１から、ストレージ装置４１０のＦＣＡ４１１の識別子であるWWNｃもしくはＰＩＤｃをアクセスできるよう

にＳＡＮ管理機構１１８に設定する。

【００１７】ついで、スイッチがゾーニング(Zoning)機能をサポートしているかを調べる（ステップＳ５）。ゾーニング機能をサポートしていない場合には、ステップＳ７にいく。また、ゾーニング(Zoning)機能をサポートしている場合には、ステップＳ６において、スイッチのゾーニング設定機構により、ゾーニング(Zoning)機能をWWNもしくはＰＩＤを使用して設定する。例えば図３の例においては、ホスト１１０のＨＢＡ１１１から、ストレージ装置４１０のＦＣＡ４１１へのアクセスはWWＮａ－WWＮｃのゾーニング設定、もしくは、ＰＩＤａ－ＰＩＤｃのゾーニング設定であり、どちらかをスイッチ３００のゾーニング設定機構３０１に設定する。

【００１８】次に、ストレージ装置がホスト・アフィニティ(Host Affinity) 機能をサポートしているかを調べる。ホスト・アフィニティ機能をサポートしていない場合には、処理を終了する。また、ホスト・アフィニティ機能をサポートしている場合には、ステップＳ８において、ホスト・アフィニティ機能により、ＦＣＡからアクセスを許可するホスト側のＨＢＡのWWNもしくはＰＩＤと領域との関係をストレージ装置のストレージ管理機構に設定し、処理を終了する。例えば図３の例においては、ホスト１１０のＨＢＡ１１１のWWＮａもしくはＰＩＤａからのコマンドをストレージ装置４１０のＦＣＡ４１１で受け付けられるように設定し、さらに、WWＮａもしくはＰＩＤａからのコマンドに対しては、領域４１５をアクセスさせるようにストレージ装置４１０のストレージ管理機構４１８に設定する。

【００１９】次に、図７のフローチャートによりスイッチ３００内のゾーニング（Zoning）設定機構３０１が行う作業について説明する。まず、ゾーニング（Zoning）設定機構３０１をゾーニング（Zoning）設定なしの状態（全てのポート間通信許可モード）に設定する（ステップＳ１）。すなわち、標準でゾーンは設定されず、全てのアクセスが許可されるようになる。次に、ゾーニング（Zoning）設定機構３０１はＳＡＮ統合管理機構５００より、全ポート間通信不許可設定を受け付け（ステップＳ２）、全ポート間通信不許可設定とする（ステップＳ３）。このように、まず全ポート間通信不許可設定とすることにより、システム起動時、アクセスパスを設定していない状態で不用意なアクセスが設定されることを防ぐことができる。

【００２０】ついで、ＳＡＮ統合管理機構５００より、ゾーン設定（ゾーンを構成するWWN群、もしくは、ＰＩＤ群）を受け付ける（ステップＳ４）。このゾーン設定は例えば、システム管理者がＳＡＮ統合管理機構５００を介して行う。上記受け付けたWWN群もしくはＰＩＤ群により、ゾーニング（Zoning）設定機構３０１に新たなゾーン(Zone)が設定される（ステップＳ５）。次にスイッチ３００は、各ポートに接続された相手ポートのWWNを確保する（ステップＳ６）。なお、ＰＩＤはスイッチ３００の物理ポート位置で決まる。ここで、ホストのポートWWＮｘより相手ポートWWＮｙへコマンドが発行されると、スイッチ３００は上記コマンド（WWＮｘ→WWＮｙ）を受け付ける（スイッチングＳ７）。そして、ゾーニング（Zoning）設定機構３０１は、WWＮｘとWWＮｙが同一ゾーン（Zone）に設定されているかを調べ（ステップＳ８）、同一ゾーンに設定されている場合には、ホストポートより相手ポートに対してコマンドを通過させる。すなわち、スイッチ３００のネームサーバ機能を用いて相手ポートを認識できるようにする（ステップＳ９）。また、同一ゾーンに設定されていない場合には、コマンドを通過させない。すなわち、スイッチ３００のネームサーバ機能を用いて相手ポート認識を削除する（ステップＳ１０）。

【００２１】次に、上記ＳＡＮ環境下におけるホストの入出力処理（Ｉ／Ｏオペレーション）の概要について説明する。以下、前記図３によりホスト１１０，１２０からＩ／Ｏオペレーションが発行された場合の処理例を説明する。なお、ここでは、ホスト１１０からＨＢＡ１１１、スイッチ３００、ＦＣＡ４１１を経由して、ストレージ４１０へのＩ／Ｏを行う場合について説明する。まず、ホスト１１０は、前記図５（ｂ）に示したストレージ・アフィニティ（Storage Affinity）テーブルより、領域４１５のアクセスはＨＢＡ１１１経由のWWＮｃを持ったＦＣＡにアクセスする必要があるということを認識する。ホスト１１０はこの情報を元にＨＢＡ１１１スイッチ３００に対しWWＮｃに対するＩ／Ｏとしてファイバチャネルフレーム発行する。

【００２２】スイッチ３００はＨＢＡ１１１より受け取ったWWＮｃに対するＩ／Ｏのファイバチャネルフレームを確保し、ＨＢＡ１１１のWWＮａとWWＮｃが、前記図５（ｃ）のスイッチ・ゾーニング（Zoning）テーブル上同一ゾーン（Zone）であることからアクセスを許可し、WWＮｃの値が設定されているＦＣＡ４１１に対してファイバチャネルフレームを転送する。ＦＣＡ４１１は受け取ったファイバチャネルフレームが、前記図５（ｄ）のホスト・アフィニティ（Host affinity ）テーブル内に設定されているWWＮａから来たものと認識できるので、これを処理することが可能と判断し、Ｉ／Ｏを実行する。

【００２３】次に上記ＳＡＮ統合管理機構５００が有する各種機能について説明する。

（１）ＳＡＮ構成設定情報との比較によるシステムの異常検出

前記したように、ＳＡＮ統合管理機構５００はＳＡＮの構成情報を個々の装置より確保して、ＳＡＮの構成設定情報５０１を格納する。また、ＳＡＮ統合管理機構５００は、定期的にもしくは、システム管理者からのコマンド指示によって、現状のＳＡＮの構成情報を読込み、Ｓ

ＡＮの構成設定情報５０１と比較して、異なっていた場合は、異常と判断してシステム管理者に通知する。例えば、前記図３の状態時にＳＡＮの構成設定情報５０１を登録し、その後ストレージ４２０の電源が落ちてしまった場合は、ＳＡＮの構成状態異常と判断して、システム管理者にストレージ４２０が見えなくなっていることを通知する。

【００２４】（２）アクセスパスの整合性の確認

ＳＡＮ統合管理機構５００は、システム管理者からのコマンド指示によって、ＳＡＮ管理機構１１８，１２８、ゾーニング（Zoning）設定機構３０１、ストレージ管理機構４１８，４２８よりアクセス関係情報を確保してアクセスパスの整合性を確認する。アクセスパスが正しく設定されていない場合は、その部分を異常とシステム管理者に通知する。この機能によりシステム管理者が勝手に個々の機器の設定を変えてしまった場合に、異常点を検出することが可能となる。また、既に、ＳＡＮがアクセスパスの設定がされた状態で存在し、新たに当該ＳＡＮ管理論理を組み込む際に、既存のＳＡＮのアクセスパスが正しく設定されているかチェックすることができる。

【００２５】（３）ＨＢＡの交換時のアクセス関係の再設定

ホスト１１０側のＨＢＡ１１１が故障して新たなＨＢＡに交換された場合、ＳＡＮ管理機構１１８はＨＢＡ交換を検知して、システム管理者に通知する。システム管理者からの構成再設定コマンドによって、ＳＡＮ管理機構１１８はＳＡＮ統合管理機構５００に交換された新しいＨＢＡのWWNを伝える。ＳＡＮ統合管理機構５００はその新しいWWNを用いてＨＢＡ交換前と同等のアクセス関係を構築し、二つのアクセス関係を設定する機構〔ゾーニング（Zoning）設定機構３０１，ストレージ管理機構４１８〕に再度アクセス関係を設定する。

【００２６】（４）ホスト交換時のアクセス関係の再設定

ホスト１１０が故障して新たなホストに交換された場合に、ホスト１１０のＳＡＮ管理機構１１８は設定がなくなっている事を検知して、システム管理者に通知する。システム管理者からの構成再設定コマンドによって、ＳＡＮ管理機構１１８はＳＡＮ統合管理機構５００に接続されているＨＢＡのWWNを伝え、ＳＡＮ統合管理機構５００は、そのWWNを用いてＨＢＡ交換前と同等のアクセス関係を構築し、二つのアクセス関係を設定する機構〔ゾーニング（Zoning）設定機構３０１，ストレージ管理機構４１８〕に再度アクセス関係を設定する。

【００２７】（５）スイッチ交換時のアクセス関係の再設定

スイッチ３００が故障して交換された際に、スイッチに設定したゾーニング（Zoning）情報がなくなっている事を検出し、システム管理者に通知する。ＳＡＮ統合管理機構５００に、システム管理者からの構成再設定コマンドによって、新しいスイッチに故障前のアクセス関係をセットさせる機構を設け、このような場合に、ＳＡＮ統合管理機構５００から、新しいスイッチに故障前のアクセス関係を再設定する。なお、スイッチ３００が故障して交換された際に、スイッチに設定したゾーニング（Zoning）情報がなくなっている事を検出するが、システム管理者には通知せず、自動的にＳＡＮ統合管理機構５００から新しいスイッチに故障前のアクセス関係をセットさせる機構をＳＡＮ統合管理機構５００に設け、再設定できるようにしてもよい。

【００２８】（６）ＦＣＡ交換時のアクセス関係の再設定

ストレージ装置側４１０のＦＣＡ４１１が故障し交換され、ＦＣＡ側のWWNが変更されてしまった場合に、これを検出しシステム管理者に通知する。システム管理者からの構成再設定コマンドによって、ストレージ管理機構４１８が新しいＦＣＡのWWNを検出してＳＡＮ統合管理機構５００に伝え、ＳＡＮ統合管理機構５００はその新しいWWNを用いてＦＣＡ交換前と同等のアクセス関係を構築し、二つのアクセス関係を設定する機構〔ＳＡＮ管理機構１１８、ゾーニング（Zonig)設定機構３０１〕に再度アクセス関係を設定する。

【００２９】（７）不用意なアクセスの設定の防止

前述したように、システム起動時にアクセスパスを設定していない状態で、不用意なアクセスが設定されることを防ぐ為に、システム起動時にアクセスパスが設定されていない状態時に、スイッチに対して全てのアクセスを許可しない設定を行う。このような設定がないと、全てのＳＡＮのストレージに対して全てのホストからアクセス出来てしまい、セキュリティ上の問題が生ずることがある。

（８）ファイバチャネルの転送クラスの設定

ファイバチャネル（ＦＣ）ではＨＢＡとＦＣＡ側で共通に設定すべきＦＣの転送クラス（Ｃｌａｓｓ）というパラメータがある。転送クラスにはクラス１～３があり、転送クラス１は殆ど使用されず、転送クラス２は転送後、アクノリッジを返し、転送クラス３は転送後、アクノリッジを返さない転送方式である。このパラメータがＨＢＡＩ側とＦＣＡ側で異なっていると転送ができない。そこで、前記したアクセスパスを設定する際に、使用するＣｌａｓｓもシステム管理者に指定させて、管理機構５００がＳＡＮ管理機構１１８，１２８、ストレージ管理機構４１８，４２８を通じて、アクセスパスを設定したＨＢＡとＦＣＡが指定された同一のＣｌａｓｓで動作させるようにする。

【００３０】次に、上記ＳＡＮ統合管理機構５００を用いたＳＡＮの障害監視について説明する。基本的にＳＡＮ統合管理機構５００を用いた場合は、ＳＡＮを構成する装置（ホスト、スイッチ、ストレージ装置）で発生し

た障害については、装置側からＳＡＮ統合管理機構５００が装置故障の報告を一括して受け取り、それをシステム管理者に報告する手法をとる。しかし、図８に示すように、ＦＣＡ４１１で障害が発生した場合、ストレージ装置４１０より、ＦＣＡ４１１が故障したという報告がＳＡＮ統合管理機構５００になされるだけでなく、スイッチ３００からもＦＣＡ４１１か、ＦＣＡ４１１に接続するスイッチポートが異常であるという報告、ホスト１１０側からのＨＢＡ１１１からのアクセスパスが使用できないという報告が入ってくる。従って、これらの３箇所の障害報告をまとめて、一つの報告としてシステム管理者に報告する手法が必要であり、以下では、この手法について説明する。

【００３１】ＳＡＮ内で障害が発生した場合は、まず、その障害報告をＳＡＮ統合管理機構５００が受け取り、システム管理者への報告を一端止める。すなわち、規定時間（例えば１分間）他の障害がＳＡＮ統合管理機構５００が管理している装置から報告されていないかどうかを待ち合わせする。待ち合わせをしている間に受け取った障害報告に関しては中身をチェックし、最初に受け取った障害との関連性がないかをＳＡＮ統合管理機構５００が保持している各アダプタのWWN，ＰＩＤや前記したアクセスパス情報から確認する。確認の結果、関連すると判断された場合は、予めＳＡＮ統合管理機構５００内で設定されている図９に示すような障害報告方法定義に従って、一つのみの障害をシステム管理者に報告し、この情報を元にシステム管理者は迅速な被擬箇所の特定を行うことができる。

【００３２】図９に上記障害報告方法定義の一例を示す。同図において、左側の欄はＳＡＮ統合管理機構５００が受け取った障害情報を示し、右側の欄はＳＡＮ総合管理機構５００が行う障害報告内容を示す。例えば、「ＦＣＡ自己エラー」と、「スイッチポートアクセスエラー」と「ホスト側アクセスエラー」という障害情報を受け取った場合、ＳＡＮ総合管理機構５００は障害報告方法定義に従い、「ＦＣＡ自己エラー」と判断して、障害報告を行う。

【００３３】以下、図１０のフローチャートにより、ＳＡＮ統合管理機構が行うＳＡＮの障害監視機能と、ＦＣＡ４１１障害報告方法の例について説明する。まず、ＳＡＮ統合管理機構５００が、障害報告を受け取る（ステップＳ１）。例えば、ＦＣＡ４１１に障害が発生した場合、ＳＡＮ統合管理機構５００は、ストレージ装置４１０よりＦＣＡ４１１の障害報告を受け取る。これにより、ＳＡＮ統合管理機構５００は、他の装置からの障害報告があるかどうかを一定時間待ち合わせる（ステップＳ２）。スイッチ側から障害報告を受け取ると（ステップＳ３）、新たな障害報告の内容と、先ほどの障害報告とのすり合わせを、WWN等の関連情報から行う（ステップＳ４）。例えば、スイッチ３００からWWNｃ，ＰＩＤｃのパスでエラー発生の報告を受け取ると、WWNｃ、ＰＩＤｃがＦＣＡ４１１のものであるため、ＳＡＮ統合管理機構５００は、同一障害であると認識する。

【００３４】次に、ホスト側からの障害報告を受け取ると（ステップＳ５）、新たな障害報告の内容と先ほどの障害報告の内容とのすり合わせをWWN等の関連情報から行う（ステップＳ６）。例えば、ホスト１１０からWWNａ，ＰＩＤａのパスでエラー発生の報告を受けると、WWNａ，ＰＩＤａとWWNｃ，ＰＩＤｃはアクセスパス６００で連携されていることをＳＡＮ統合管理機構５００は認識しているため、同一障害と認識する。上記待ち合わせを一定時間行い（ステップＳ７）、一定時間待ち合わせると、関連情報をすり合わせた結果、障害の根本原因を特定する（ステップＳ８）。根本原因の特定方法はＳＡＮ統合管理機構５００に含まれる前記障害報告定義によって行われる。例えば、スイッチ３００側の障害とホスト側の障害は、上記障害報告定義により、ストレージ側のＦＣＡ障害と判断する。

【００３５】根本原因が特定されると、根本原因のみをシステム管理者に報告する（ステップＳ９）。例えば、前記したＦＣＡ４１１障害の場合には、ＦＣＡ４１１障害のみをシステム管理者に報告する。上記説明では、被擬箇所を報告するだけであったが、これだけでなく、関連して報告された被擬箇所と判定されなかった報告も、関連障害として報告するようにしてもよい。これにより、影響範囲をシステム管理者は特定できることとなる。

【００３６】また、予め、ＳＡＮ統合管理機構５００が、各アクセスパスの設定情報だけでなく各アクセスパスで使用しているホスト側の論理ボリュームの情報もホスト側のＳＡＮ管理機構１１８から確保し、ＳＡＮ構成設定情報５０１に格納しておけば、障害影響のある論理ボリュームをシステム管理者に報告することができる。すなわち、ＳＡＮ統合管理機構５００は、ＳＡＮ内から障害が報告されると、その故障箇所を使用しているアクセスパスをＳＡＮ統合管理機構５００内のＳＡＮ構成設定情報５０１から取り出す。さらに、そのアクセスパスを使用しているホスト論理ボリュームを取り出し、障害影響のある論理ボリュームをシステム管理者に報告する。例えば、ＦＣＡ４１１障害の場合には、領域４１５は使用不可であることを報告する。システム管理者は、障害影響のある論理ボリュームがわかると、すぐさまその論理ボリュームのリカバリが可能であり、業務影響を最小限にさせることが実現できる。

【００３７】（付記１）複数のホストコンピュータと複数のストレージ装置が、スイッチを介して接続されたストレージエリア・ネットワーク・システムにおいて、
上記ストレージエリア・ネットワークを統合制御する統合管理機構を備え、該統合管理機構はホストコンピュータとストレージ装置とのアクセス経路情報を備えるとと

もに、該アクセス経路情報に基づき、ホストコンピュータのストレージエリア・ネットワーク管理機構に対して、ストレージ装置に対する管理情報を通知し、スイッチの領域設定機構に対して領域情報を通知し、ストレージ装置のストレージ管理機構に対して上記ホストコンピュータについてのアクセス制限情報を通知することを特徴とするストレージエリア・ネットワーク管理システム。

（付記２）上記統合管理機構は、ストレージエリア・ネットワークの構成状態を個々の装置より取得して、ストレージエリア・ネットワークの構成設定情報として保持し、定期的もしくは、システム管理者からの指示によって、現状のストレージエリア・ネットワークの構成状態を集収し、上記構成設定情報と集収した現状の構成情報とを比較することにより、ストレージエリア・ネットワーク・システムの異常を判断することを特徴とする付記１のストレージエリア・ネットワーク管理システム。

（付記３）上記統合管理機構は、ホストコンピュータのストレージエリア・ネットワーク管理機構、スイッチ、および／またはストレージ装置より、アクセス関係情報を取得して、アクセスパスの整合性を確認し、アクセスパスが正しく設定されていないとき、その部分を異常として通知することを特徴とする付記１または付記２のストレージエリア・ネットワーク管理システム。

（付記４）複数のホストコンピュータと複数のストレージ装置が、スイッチを介して接続されたストレージエリア・ネットワーク・システムであって、上記ストレージエリア・ネットワークを統合制御する統合管理機構を備え、該統合管理機構はホストコンピュータとストレージ装置とのアクセス経路情報を備えるとともに、該アクセス経路情報に基づき、ホストコンピュータのストレージエリア・ネットワーク管理機構に対して、ストレージ装置に対する管理情報を通知し、スイッチの領域設定機構に対して領域情報を通知し、ストレージ装置のストレージ管理機構に対して上記ホストコンピュータについてのアクセス制限情報を通知するストレージエリア・ネットワーク管理システムにおいて、ホストコンピュータ、ホストコンピュータに設けられたホストバス・アダプタ、スイッチ、あるいは、ストレージ装置に設けられたファイバチャネル・アダプタが交換されたとき、上記統合管理機構はこれを検知し、上記ホストコンピュータのストレージエリア・ネットワーク管理機構、スイッチの領域設定機構、もしくは、ストレージ装置のストレージ管理機構から、交換後の設定情報を取得し、交換前と同等のアクセス関係を構築するように再度アクセス関係を設定することを特徴とするストレージエリア・ネットワーク・システム。

（付記５）ホストコンピュータのホストバス・アダプタが故障して交換された際、統合管理機構はホストバス・アダプタの交換を検知して、システム管理者に通知し、システム管理者からの構成再設定コマンドにより、統合管理機構１は、ホストコンピュータのストレージエリア・ネットワーク管理機構に交換された新しいホストバス・アダプタの設定情報を伝え、該新しい設定情報を用いてホストバス・アダプタ交換前と同等のアクセス関係を構築し、ストレージエリア・ネットワーク管理機構、領域設定機構、ストレージ管理機構に再度アクセス関係を設定することを特徴とする付記４記載のストレージエリア・ネットワーク・システム。

（付記６）ホストコンピュータが故障して交換された際、統合管理機構は、ホストコンピュータのストレージエリア・ネットワーク管理機構の設定がなくなっている事を検知して、システム管理者に通知し、システム管理者からの構成再設定コマンドにより、上記ストレージエリア・ネットワーク管理機構は統合管理機構に対して接続されているホストバス・アダプタの設定情報を伝え、統合管理機構はその情報を用いてホストコンピュータ交換前と同等のアクセス関係を構築し、領域設定機構、ストレージ管理機構に再度アクセス関係を設定することを特徴とする付記４記載のストレージエリア・ネットワーク・システム。

（付記７）スイッチが故障して交換された際、統合管理機構は、スイッチに設定した領域設定情報がなくなっている事を検出し、システム管理者に通知し、システム管理者からの構成再設定コマンドによって、新しいスイッチに故障前のアクセス関係をセットさせ、アクセス関係を再設定できるようにしたことを特徴とする付記４記載のストレージエリア・ネットワーク・システム。

（付記８）スイッチが故障して交換された際に、スイッチに設定した領域設定情報がなくなっている事を検出し、統合管理機構は、自動的に新しいスイッチに故障前のアクセス関係をセットさせ、アクセス関係を再設定できるようにしたことを特徴とする付記４記載のストレージエリア・ネットワーク・システム。

（付記９）ストレージ装置側のファイバチャネル・アダプタ交換され、ファイバチャネル・アダプタの設定情報が変更された場合、統合管理機構は、これを検出し、システム管理者に通知し、システム管理者からの構成再設定コマンドによって、ストレージ管理機構が新しい設定情報を統合管理機構に伝え、統合管理機構はその新しい設定情報を用いて交換前と同等のアクセス関係を構築し、ストレージエリア・ネットワーク管理機構、領域設定機構に再度アクセス関係を設定することを特徴とする付記４記載のストレージエリア・ネットワーク・システム。

（付記１０）複数のホストコンピュータと複数のストレージ装置が、スイッチを介して接続されたストレージエリア・ネットワーク・システムであって、上記ストレージエリア・ネットワークを統合制御する統合管理機構を備え、該統合管理機構はホストコンピュータとストレー

ジ装置とのアクセス経路情報を備えるとともに、該アクセス経路情報に基づき、ホストコンピュータのストレージエリア・ネットワーク管理機構に対して、ストレージ装置に対する管理情報を通知し、スイッチの領域設定機構に対して領域情報を通知し、ストレージ装置のストレージ管理機構に対して上記ホストコンピュータについてのアクセス制限情報を通知するストレージエリア・ネットワーク管理システムにおいて、システム起動時であって、アクセス経路情報が設定されていない状態の時に、上記統合管理機構はスイッチの領域設定機構に対して全てのアクセスを許可しない設定を行い、その後スイッチの領域設定機構に対して領域設定を行うことを特徴とするストレージエリア・ネットワーク・システム。

（付記１１）複数のホストコンピュータと複数のストレージ装置が、スイッチを介して接続されたストレージエリア・ネットワーク・システムであって、上記ストレージエリア・ネットワークを統合制御する統合管理機構を備え、該統合管理機構はホストコンピュータとストレージ装置とのアクセス経路情報を備えるとともに、該アクセス経路情報に基づき、ホストコンピュータのストレージエリア・ネットワーク管理機構に対して、ストレージ装置に対する管理情報を通知し、スイッチの領域設定機構に対して領域情報を通知し、ストレージ装置のストレージ管理機構に対して上記ホストコンピュータについてのアクセス制限情報を通知するストレージエリア・ネットワーク管理システムにおいて、上記統合管理機構は、指定されたファイバチャネルの転送クラスを、アクセス経路情報を設定したホストコンピュータのストレージエリア・ネットワーク管理機構、ストレージ装置のストレージ管理機構を介して設定し、ホストコンピュータのホストバス・アダプタ、ストレージ装置のファイバチャネル・アダプタを同一の転送クラスで動作させることを特徴とするストレージエリア・ネットワーク・システム。

（付記１２）複数のホストコンピュータと複数のストレージ装置が、スイッチを介して接続されたストレージエリア・ネットワーク・システムであって、上記ストレージエリア・ネットワークを統合制御する統合管理機構を備え、該統合管理機構はホストコンピュータとストレージ装置とのアクセス経路情報を備えるとともに、該アクセス経路情報に基づき、ホストコンピュータのストレージエリア・ネットワーク管理機構に対して、ストレージ装置に対する管理情報を通知し、スイッチの領域設定機構に対して領域情報を通知し、ストレージ装置のストレージ管理機構に対して上記ホストコンピュータについてのアクセス制限情報を通知するストレージエリア・ネットワーク管理システムにおいて、ストレージエリア・ネットワーク・システム内で障害が発生した際、上記統合管理機構は、障害報告を受け取り、規定時間の間、他の障害が報告されているか否かを待ち合わせ、その間に受け取った障害報告をチェックして、最初に受け取った障害報告との関連性を調べ、関連性があると判断されたとき、予め上記統合管理機構内で設定されている障害報告方法定義に従って、１つの障害箇所のみを報告することを特徴とするストレージエリア・ネットワーク・システム。

（付記１３）１つの障害箇所に加えて、受け取った関連する障害報告を関連障害として報告することを特徴とする付記１２記載のストレージエリア・ネットワーク・システム。

（付記１４） 上記統合管理機構は、各アクセス経路情報の設定情報に加えて、各アクセスパスで使用しているホスト側の論理ボリュームの情報をホストコンピュータのストレージエリア・ネットワーク管理機構から取得して保持し、ストレージエリア・ネットワーク・システム内から障害が報告されたとき、該障害箇所を使用しているアクセス経路情報に基づき、該アクセスパスを使用している論理ボリュームを取り出し、障害影響のある論理ボリュームを報告することを特徴とする付記１２記載のストレージエリア・ネットワーク・システム。

（付記１５）複数のホストコンピュータと複数のストレージ装置が、スイッチを介して接続され、これらを統合管理する統合管理機構を備えたストレージエリア・ネットワーク・システムにおけるホストコンピュータであって、上記ホストコンピュータのストレージエリアネットワーク管理機構は、上記統合管理機構から通知されるストレージ装置に対する管理情報に基づきストレージ装置に対するアクセス情報を設定することを特徴とするストレージエリア・ネットワーク・システムにおけるホストコンピュータ。

（付記１６）複数のホストコンピュータと複数のストレージ装置が、スイッチを介して接続され、これらを統合管理する統合管理機構を備えたストレージエリア・ネットワーク・システムにおけるスイッチであって、上記スイッチの領域設定機構は、上記統合管理機構から通知される領域情報に基づき領域設定を行うことを特徴とするストレージエリア・ネットワーク・システムにおけるスイッチ。

（付記１７）複数のホストコンピュータと複数のストレージ装置が、スイッチを介して接続され、これらを統合管理する統合管理機構を備えたストレージエリア・ネットワーク・システムにおけるストレージ装置であって、上記ストレージ装置のストレージ管理機構は、上記統合管理機構から通知されるアクセス制限情報に基づき、ストレージに対するアクセス制限条件を設定することを特徴とするストレージエリア・ネットワーク・システムにおけるストレージ装置。

（付記１８）複数のホストコンピュータと複数のストレージ装置が、スイッチを介して接続されたストレージエリア・ネットワーク・システムを統合管理する統合管理機構であって、上記統合管理機構は、ホストコンピュー

タのストレージエリア・ネットワーク管理機構に対して、ストレージ装置に対する管理情報を通知し、スイッチの領域設定機構に対して領域情報を通知し、ストレージ装置のストレージ管理機構に対して上記ホストコンピュータについてのアクセス制限情報を通知することを特徴とするストレージエリア・ネットワーク・システムにおける統合管理機構。

（付記１９）複数のホストコンピュータと複数のストレージ装置が、スイッチを介してファイバチャネルで接続されたストレージエリア・ネットワーク・システムを統合制御する統合管理プログラムであって、上記統合管理プログラムは、ホストコンピュータとストレージ装置とのアクセス経路情報に基づき、ホストコンピュータのストレージエリア・ネットワーク管理機構に対して、ストレージ装置に対する管理情報を通知する処理と、スイッチの領域設定機構に対して領域情報を通知する処理と、ストレージ装置のストレージ管理機構に対して上記ホストコンピュータについてのアクセス制限情報を通知する処理とをコンピュータに実行させ、ホストとストレージとのアクセス関係を一括して管理することを特徴とするストレージエリア・ネットワーク・システムを統合制御するプログラム。

（付記２０）複数のホストコンピュータと複数のストレージ装置が、スイッチを介してファイバチャネルで接続されたストレージエリア・ネットワーク・システムを統合制御する統合管理プログラムを記録した記録媒体であって、上記統合管理プログラムは、ホストコンピュータとストレージ装置とのアクセス経路情報に基づき、ホストコンピュータのストレージエリア・ネットワーク管理機構に対して、ストレージ装置に対する管理情報を通知し、スイッチの領域設定機構に対して領域情報を通知し、ストレージ装置のストレージ管理機構に対して上記ホストコンピュータについてのアクセス制限情報を通知し、ホストとストレージとのアクセス関係を一括して管理することを特徴とするストレージエリア・ネットワーク・システムを統合制御するプログラムを記録した記録媒体。

【００３８】

【発明の効果】以上説明したように、本発明においては、ＳＡＮにストレージエリア・ネットワークを統合制御する統合管理機構を設け、ホストとストレージとのアクセス関係を上記統合管理機構により一括して管理するようにしたので、以下の効果を得ることができる。

（１）信頼性の高い一元管理されたＳＡＮシステムを構築することができる。また、前記したホスト・アフィニティ、ゾーニング等の機能を持っていない、過去のシステムに対しても対応できるので、全て新しいシステムを購入してＳＡＮを構築することが動作環境の必須条件とならない。

（２）ＳＡＮの異常や、アクセスパスの整合性を容易に確認することができる。

（３）ＳＡＮを構成するホスト、ＨＡＢ、スイッチ、ストレージ装置、ＦＣＡ等が交換され、ＳＡＮの構成状態が変更されても容易に対応することができる。

（４）ＳＡＮに異常が発生した場合、被疑箇所やその影響範囲を容易に特定することができ、業務影響を最小限に止めることができる。

【図面の簡単な説明】

【図１】本発明の概要を説明する図である。

【図２】本発明の対象となるＳＡＮシステムの構成例を示す図である。

【図３】本発明の実施例のＳＡＮ管理システムの構成を示す図である。

【図４】ストレージ装置のハードウェア構成例を示す図である。

【図５】アクセスパス設定情報、ストレージ・アフィニティ・テーブル、スイッチ・ゾーニングテーブル、ホスト・アフィニティ・テーブルの例を示す図である。

【図６】ＳＡＮ統合管理機構が行う処理のフローチャートを示す図である。

【図７】ゾーニング設定機構が行う処理のフローチャートを示す図である。

【図８】ＳＡＮの障害管理を説明する図である。

【図９】障害報告方法定義の一例を示す図である。

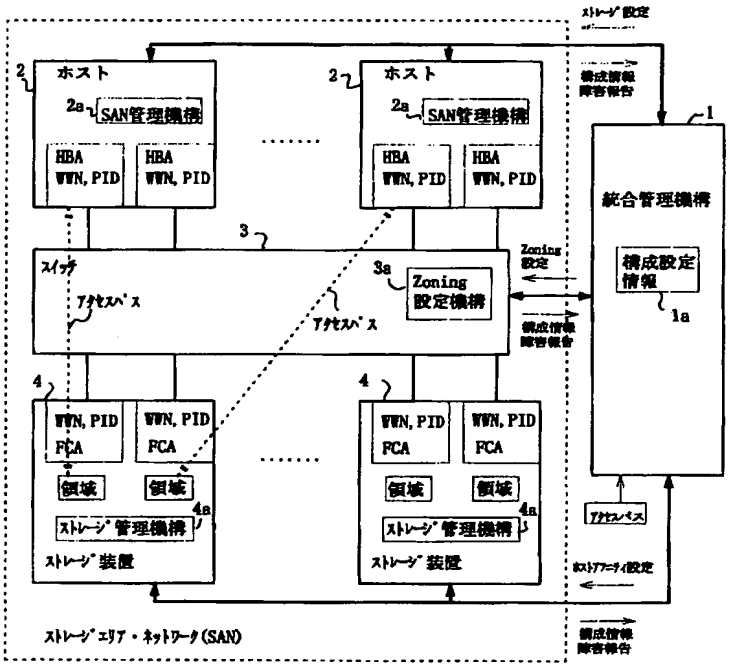
【図１０】ＳＡＮ統合管理機構が行うＳＡＮの障害監視機能のフローチャートである。

【符号の説明】

１	統合管理機構
１ａ	構成設定情報
２	ホスト
２ａ	ＳＡＮ管理機構
３	スイッチ
３ａ	ゾーニング(Zoning)設定機構
４	ストレージ装置
４ａ	ストレージ管理機構
１１０，１２０	ホスト
１１１，１１２	ホストバス・アダプタ（ＨＢＡ）
１２１	ホストバス・アダプタ（ＨＢＡ）
３００	スイッチ
３０１	ゾーニング設定情報
４１０，４２０	ストレージ装置
４１１，４２１	ファイバチャネル・アダプタ（ＦＣＡ）
４２１	ファイバチャネル・アダプタ（ＦＣＡ）
４１８，４２８	ストレージ管理機構
５００	ＳＡＮ統合管理機構
５０１	ＳＡＮ構成設定情報

【図１】

本発明の概要を説明する図



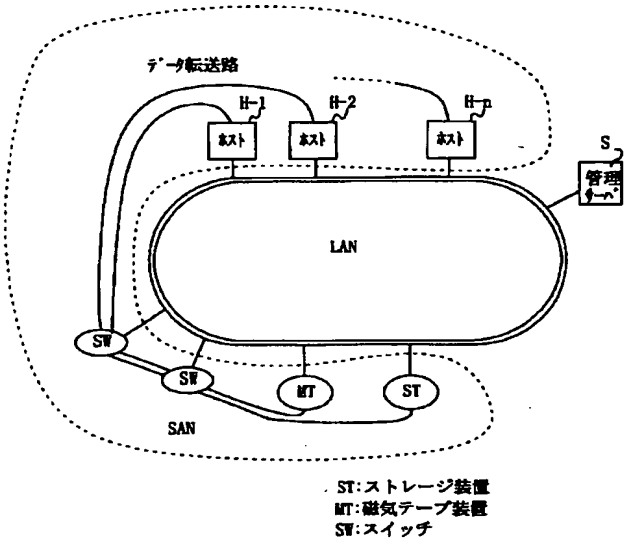
【図９】

障害報告方法定義の一例を示す図

受け取った障害情報	障害報告内容
FCA自己エラー＋スイッチポートエラー＋ホスト側アクセスパスエラー スイッチポートエラー＋ホスト側アクセスパスエラー ：	FCA自己エラー スイッチポートエラー ：

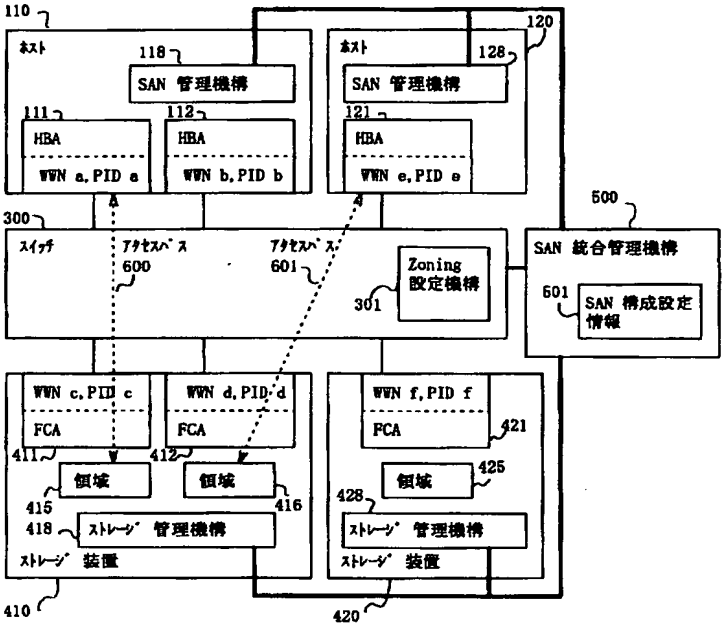
【図２】

本発明の対象となるＳＡＮシステムの構成例を示す図



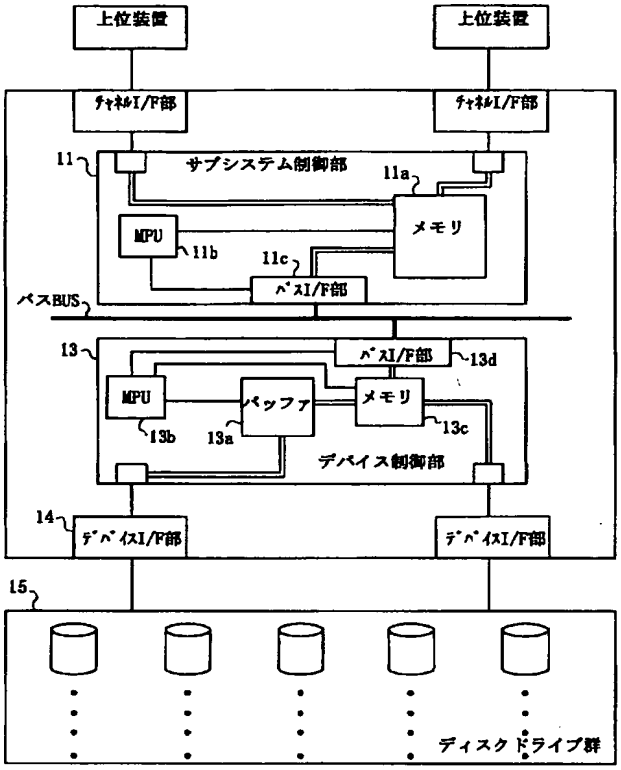
【図３】

本発明の実施例のＳＡＮ管理システムの構成を示す図



【図４】

本発明の実施例のストレージ装置のハードウェア構成例を示す図



【図５】

アクセスパス設定情報、ストレージ・アフィニティ・テーブル、
スイッチ・ゾーニングテーブル、ホスト・アフィニティ・テーブル
の例を示す図

(a)SAN統合管理機構内のアクセスパス設定情報

ｱｸｾｽﾊﾟｽ	ホスト	HBA(WWN, PID)	ｽﾄﾚｰｼﾞ装置	FCA(WWN, PID)	領域
600	110	111(WWNa, PIDa)	410	411(WWNc, PIDc)	415
601	120	121(WWNb, PIDa)	410	412(WWNd, PIDd)	416

(b)Storage Affinityテーブル(ﾎｽﾄ110の場合)

HBA	アクセス先FCAの情報	FCA配下のアクセスする領域
111	WWN c	415
112	なし	なし

(c)ｽｲｯﾁZoningテーブル(ｽｲｯﾁ300場合)

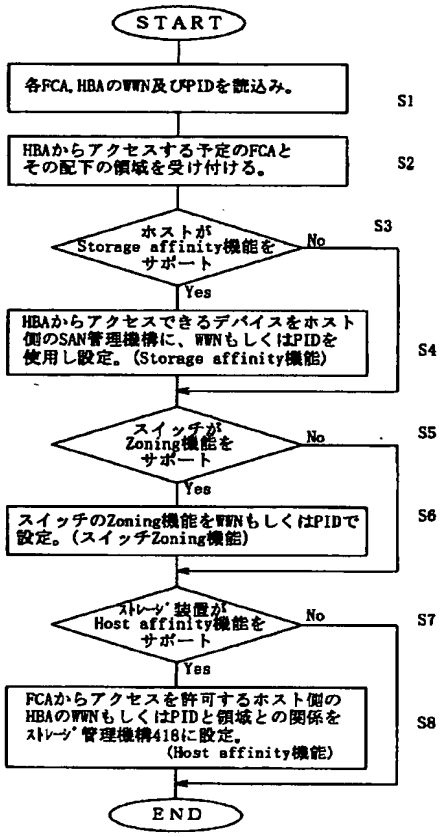
Zone名	Zoning設定
A	WWN a, WWN c
B	WWN e, WWN d

(d)Host Affinityテーブル(ストレージ410の場合)

FCA	アクセス許可HBAの情報	対応する領域
411	WWN a	415
412	WWN e	416

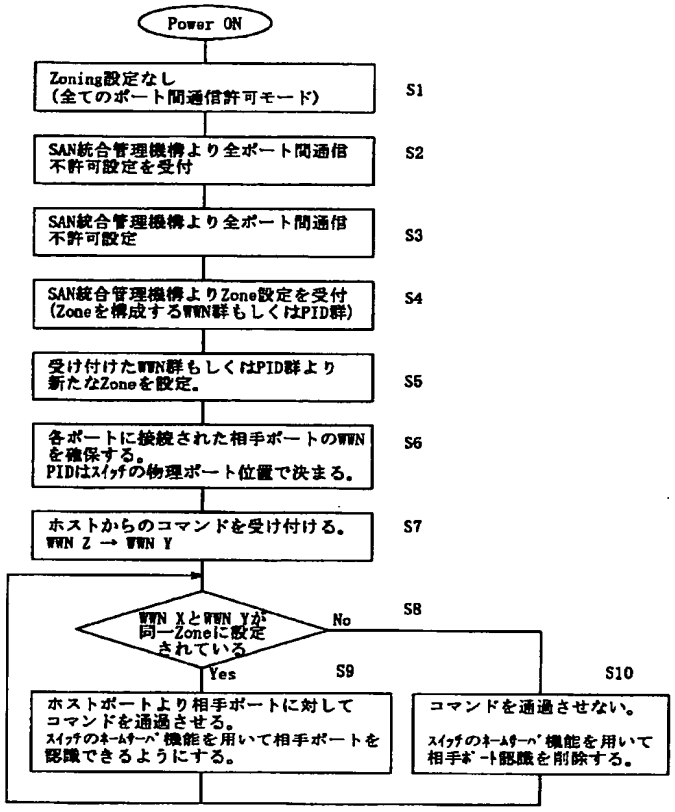
【図６】

ＳＡＮ統合管理機構が行う処理のフローチャートを示す図



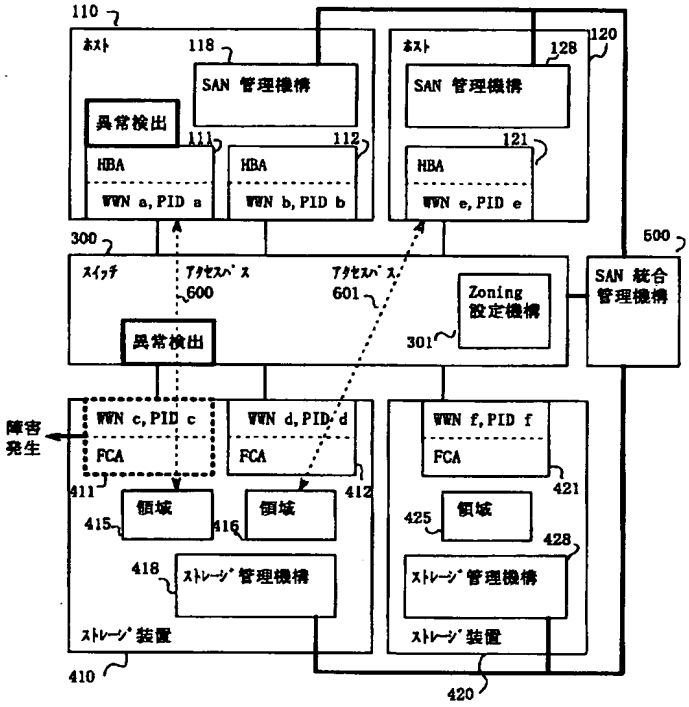
【図７】

ゾーニング設定機構が行う処理のフローチャートを示す図



【図８】

ＳＡＮの障害管理を説明する図



【図１０】

ＳＡＮ統合管理機構が行うＳＡＮの障害監視機能のフローチャート